Claims

1. A method for monitoring events generated on at least one computer system, said method comprising the steps of:

(a) monitoring a set of event data generated on said at least one system;

(b) recording said set of event data in a database;

(c) interrogating said database to thereby select alert event data from said set of event data according to a predefined set of rules; and

(d) reading said alert event data and issuing an appropriate action due to said generated event, said action issued according to said predefined set of rules.

2. A method as claimed in claim 1, wherein said action response occurs in real-time as a user interacts with said computer system.

3. A method as claimed in claim 2, wherein said method further comprises the step of:

(e) issuing said action response to said at least one computer system to prevent further interaction of said user with said computer system.

4. A method as claimed in claim 1, wherein before step (b) said method further includes the step of:

(f) parsing event data having one data format and reformatting said data into another common data format.

5 A method as claimed in claim 1, wherein said set of event data is monitored from the interaction of one or more users interaction with one or more computers on a network.

6. A method as claimed in claim 5, wherein said monitored set of event data is monitored from a number of sources on said computer network, including any one or more of the following network components: the application program layer; the transport layer; security layer; operating system.

7. A method as claimed in claim 6, wherein said application program layer includes any one or more the following: customer relationship management, enterprise resource planning; customer billing.

8. A method as claimed in claim 6, wherein said operating system includes any one or more but not limited to the following: database application server; LAN; router; PABX; telephone network; network server.

9 A method as claimed in claim 6, wherein said security layer includes any one or more but not limited to the following: firewalls; card-swipe facility access; close-circuit security television.

10. A method as claimed in claim 1. wherein said method further includes the step of:

(g) permitting an authorised user to interactively define said set of rules in step (c).

11. A method as claimed in claim 10, wherein said authorised user can interactively define and/or amend said set of rules in step (c) using a user graphical interface.

12. A method as claimed in claim 11, wherein said graphical interface is a web browser.

13. A method as claimed in claim 1, wherein said method further includes the step of:

(h) determining said action response based upon said pre-defined set of rules and based upon a weighting factor applied to recorded historical outcomes for monitored events.

14. A method as claimed in claim 1, wherein one or more agent programs are provided on at least one computer of said computer system to thereby monitor said set of event data.

15. A method as claimed in claim 1, wherein said event data is recorded in a relational database.

16. A method as claimed in claim 15, wherein said event data is assigned a unique log identifier in said database to identify the record of each event.

17. A method as claimed in claim 16, wherein said unique log identifier is used to correlated as a single event, a multiplicity of events generated on one or more computer systems.

18. A method as claimed in claim 1, wherein a report is generated to report said recorded said set of event data.

19. A method as claimed claim 1, wherein said appropriate action is a message sent to a network administrator.

20. A method as claimed in claim 19, wherein said appropriate action is a message sent to an authorised person.

21. A method as claimed in claim 20, wherein said message is any one or more of the following message types: electronic mail; SMS text massaging; audio signal; telephone call; pagers; WAP appliances.

22. A computer memory storing thereon an application program for controlling the execution of a processor to monitor events generated on at least one computer system, the computer program controlling the processor to:

monitor a set of event data generated on at least one computer system;

record said set of event data in a database;

interrogate said database to thereby select alert event data from said set of event data according to a predefined set of rules; and

read said alert event data and issue an appropriate action due to said generated event on said computer system, said action issued according to said predefined set of rules.

23. A computer memory as claimed in claim 22, wherein said action response occurs in real-time.

24. A computer memory as claimed in claim 22, wherein the computer program further controls the processor to issue said action response to said at least one computer system to prevent further interaction a user of said computer.

25. A computer memory as claimed in claim 22, wherein before recording said set of event data in a database, the computer program further controls the processor to parse event data having one data format and reformat said data into another common data format.

26 A computer memory as claimed in claim 22, wherein said set of event data is monitored from events generated by one or more computers on a network.

27. A computer memory as claimed in claim 26, wherein said monitored set of event data is monitored from a number of sources on said computer network, including any one or more of the following network components: the application program layer; the transport layer; security layer; operating system.

28. A computer memory as claimed in claim 27, wherein said application program layer includes any one or more of the following: customer relationship management, enterprise resource planning; customer billing.

29. A computer memory as claimed in claim 27, wherein said operating system includes any one or more of the following: database application server; LAN; router; PABX; telephone network; network server.

30 A computer memory as claimed in claim 27, wherein said security layer includes any one or more of the following: firewalls; card-swipe facility access; close-circuit security television.

31. A computer memory as claimed in claim 22, wherein said computer program further controls the processor to permit an authorised user to interactively define said set of rules.

32. A computer memory as claimed in claim 31, wherein said authorised user can define and/or amend said set of rules in step using a user graphical interface.

33. A computer memory as claimed in claim 32, wherein said graphical interface is a web browser.

34. A computer memory as claimed in claim 22, wherein said computer program further controls the processor to determine said action response based upon said pre-defined set of rules and based upon a weighting factor applied to recorded historical outcomes for monitored events.

35. A computer memory as claimed in claim 22, wherein one or more agent programs are provided on each computer system to monitor said set of event data.

36. A computer memory as claimed in claim 22, wherein said event data is recorded in a relational database.

37. A computer memory as claimed in claim 36, wherein said event data is assigned a unique log identifier in said database to identify the record of each event.

38. A computer memory as claimed in claim 37, wherein said unique log identifier is used to correlated as a single event, a multiplicity of events generated on one or more computer systems.

39. A computer memory as claimed in claim 22, wherein a report is generated to report said recorded set of event data.

40. A computer memory as claimed claim 22, wherein said appropriate action is a message sent to a network administrator.

41. A computer memory as claimed in claim 40, wherein said appropriate action is a message sent to an authorised person.

42. A computer memory as claimed in claim 41, wherein said message is any one or more of the following message types: electronic mail; SMS text massaging; audio signal; telephone call; pagers; WAP appliances.

43. A monitoring system for monitoring events generated on at least one computer system, said monitoring system comprising

one ore more agent programs for monitoring a set of event data generated on said at least one computer system;

a database for recording said set of event data in a database, said database adapted to be interrogated to thereby select alert event data from said set of event data according to a predefined set of rules; and

action generation means for reading said alert event data and issuing an appropriate action to said generated event on said computer system, said action being issued according to said predefined set of rules.

44. A monitoring system as claimed in claim 43, wherein said action generation means issues said action response to said at least one computer system to prevent interaction of a user with said computer.

45. A monitoring system as claimed in claim 43, wherein before recording said event data in said database, said event data having one data format is parsed and reformatting into another common data format.

46. A monitoring system as claimed in claim 43, wherein an authorised user is able to define said set of rules.

47. A method for monitoring events generated on a computer network, said method comprising the steps of:

(a) monitoring a set of event data generated by a plurality of nodes on said computer network in a plurality of data formats;

(b) parsing said monitored set of event data in a plurality of data formats;

(c) converting said parsed set of event data from said plurality of data formats into a common format;

(d) recording said set of event data in a common format into one or more databases;

(e) interrogating said database to thereby select alert event data from said set of event data according to a predefined set of rules.

48. A method as claimed in claim 47, wherein said method further comprises the step of:

(f) reading said alert event data and issuing an appropriate action due to a user's interaction with or system generated event on a computer, said action issued according to said predefined set of rules.

49. A computer memory storing thereon an application program for controlling the execution of a processor to monitor events generated on a computer network, said processor coupled to said computer network and said computer program controlling the processor to:

monitor a set of event data generated by a plurality of nodes on said computer network, event data of said monitored set of event data being in a multiplicity of data formats;

parse said monitored set of event data in a multiplicity of data formats;

convert said parsed set of event data from said multiplicity of data formats into a common format;

record said set of event data in a common format into one or more databases;

interrogate said database to thereby select alert event data from said set of event data according to a predefined set of rules.

50. A computer program as claimed in claim 49, wherein said computer program controls the processor to read said alert event data and thereby issue an appropriate action due to said user's interaction with or system generated event on said computer, said action issued according to said predefined set of rules.

51. A method for monitoring events generated on a distributed computer network, said distributed computer network having a plurality of node clusters, said node clusters consisting of a plurality of nodes arranged to exchange data with a master node, said master node adapted to exchange data with other master nodes of said node clusters, said method comprising the steps of:

for each node cluster

(a) monitoring event data generated by said nodes within said cluster;

(b) recording said event data in at leasc one database assigned to said node cluster; and

in a local cluster

(f) interrogating said database to thereby select event data which satisfies interrogation criteria; and

if no event data satisfies interrogation criteria in step (f)

(g) interrogating other node clusters to thereby select event data which satisfies said interrogation criteria.

52. A method for monitoring events generated on a distributed computer network, said distributed computer network having a plurality of node clusters, said node clusters consisting of a plurality of nodes arranged to exchange data with a master node, said master node adapted to exchange data with other master nodes of other node clusters, said method comprising the steps of:

for each node cluster

(a) monitoring event data generated by said nodes within said cluster;

(b) recording said event data in at lease one database assigned to said node cluster;

(c) assigning a unique identifier to identify an event type for said recorded event data;

in a local cluster

(f) interrogating said database to thereby selcct event data which satisfies interrogation criteria;

(g) reading said unique identifier of selected event data in (f); and

in other clusters

(h) interrogating said other node clusters to determine if a correlation exists with said read unique identifier.

53. A method for monitoring events resulting from interaction of a user with at least one computer or system generated event, substantially according to any one of the examples described herein with reference to the accompanying drawings.

54. A computer memory storing thereon an application program for controlling the execution of a processor to monitor events resulting from interaction of a user with at least one computer, substantially according to any one of the examples described herein with reference to the accompanying drawings.

55. A monitoring system for monitoring events resulting from interaction of a user with or system generated event on at least one computer, substantially as herein described with reference to the accompanying drawings.